What is Public Key Encryption?

Public key encryption is an encryption which uses two keys: public and private keys.

The public key is made known to anyone who wants to communicate with the computer, while the private key is known only by the receiving computer.

Data encrypted using the public key can be decrypted using the private key, and vice versa.

A famous implementation of public key encryption is the SSL (Secure Socket Layer).

Historical facts

- Public key algorithm was first invented by Clifford Cocks in the early 1970s.
- The RSA algorithm, was invented by Rivest, Shamir and Adleman, and was published in 1976.
- In 1984, Taher ElGamal invented the ElGamal algorithm.
- In 1989, Koblitz developed his hyperelliptic curve cryptography algorithm, which was not very effective.

Public Key Encryption

Presented by:
Charlene Aquilina
B.Ed. Computing 3rd year
2004—2005

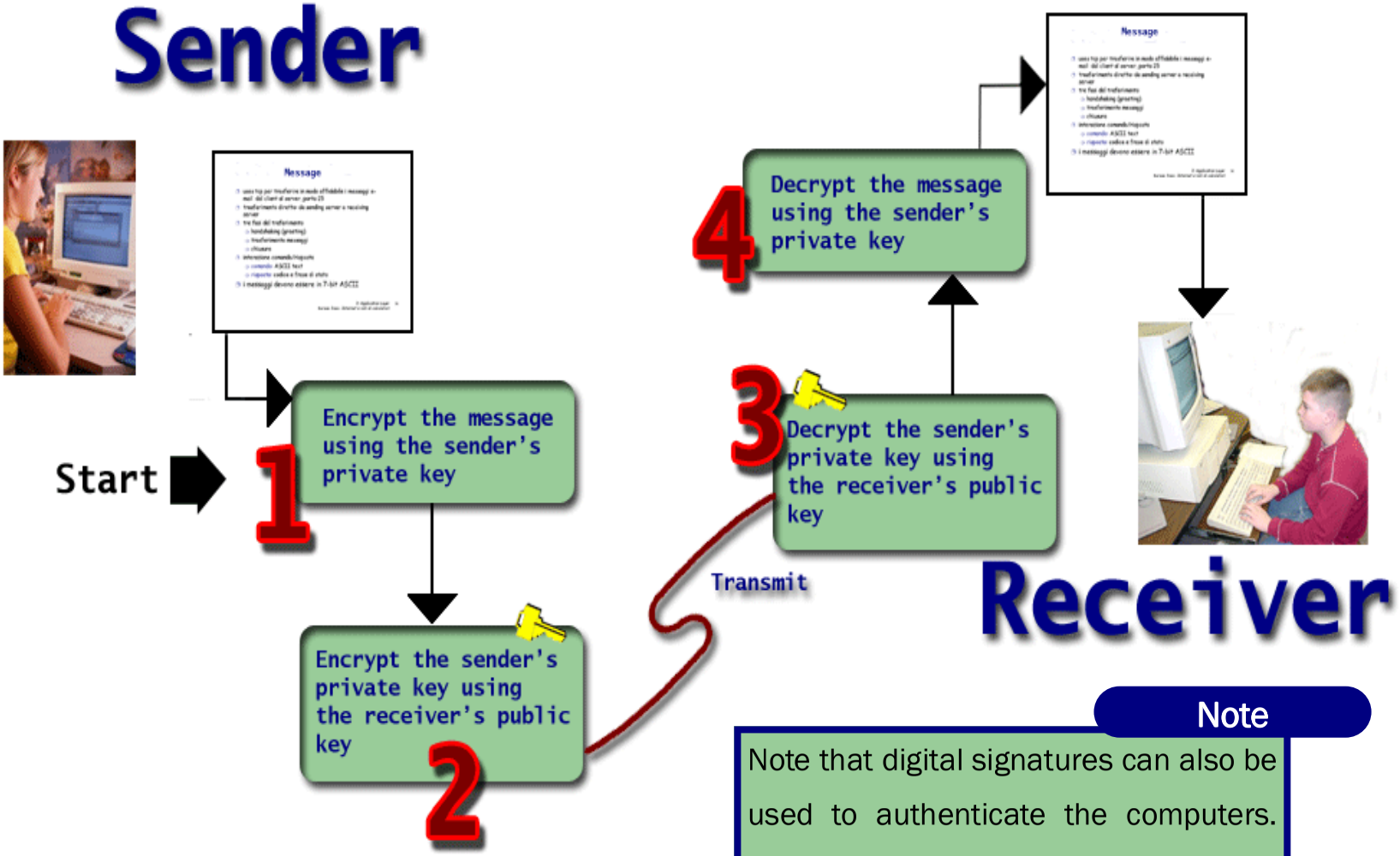
For further reference visit:

http://www.geocities.com/publickeyencryption

How does Public Key Encryption work?

Main Steps

1. Sender encrypts message using its private key.
2. Sender encrypts its private key using the receiver's public key.
3. Receiver decrypts the sender's private key using its private key.
4. Receiver decrypts the message using the sender's private key.



Note

Note that digital signatures can also be used to authenticate the computers. This is done to ensure that the computers are who they say they are.